

Useful entanglement can be extracted from all nonseparable states

Lluís Masanes

School of Mathematics, University of Bristol, Bristol BS8 1TW, U.K.

(Dated: October 8, 2008)

We consider entanglement distillation from a single-copy of a multipartite state, and instead of rates we analyze the “quality” of the distilled entanglement. This “quality” is quantified by the fidelity with the GHZ-state. We show that each not fully-separable state σ can increase the “quality” of the entanglement distilled from other states, no matter how weakly entangled is σ . We also generalize this to the case where the goal is distilling states different than the GHZ. These results provide new insights on the geometry of the set of separable states and its dual (the set of entanglement witnesses).

I. INTRODUCTION

Quantum Information Science studies the possibilities and advantages in using quantum physical devices for information processing tasks. Some of these tasks require noiseless entanglement as a principal ingredient [1]. Real devices are noisy and not isolated from the environment, therefore they usually cannot be described by pure states. Entanglement distillation is the process of transforming noisy into noiseless entanglement by using only *local operations and classical communication* (LOCC) [2]. In the most studied scenario, one has an arbitrarily large number of copies of a state and wants to know at which rate singlets can be obtained. *Bound entangled states* are the ones that cannot be distilled, and its existence is proven in [3].

In this paper we generalize the results of [4] to states with an arbitrary number of parties. However, as explained in what follows, this generalization is made in the strongest possible way. In the multipartite scenario the entanglement present in a particular state is not necessarily shared among all parties. Here we call entangled any state ρ that is not fully-separable, that is

$$\rho \neq \sum_k \varrho_1^k \otimes \cdots \otimes \varrho_N^k, \quad (1)$$

where ϱ_n^k are positive semi-definite matrices. We show that all entangled (i.e. not fully-separable) states have some extractable GHZ-like entanglement [5]. This provides a very simple picture of quantum correlations, in which all kinds of entanglement (independent of the number of parties they involve) are, in a sense, fungible.

II. SINGLE-COPY DISTILLATION SCENARIO

Given an arbitrary N -partite state ρ (acting on $\mathcal{H} = \bigotimes_n^N \mathcal{H}_n$) we consider the states $\tilde{\rho}$ acting on $\mathcal{K} = \bigotimes_n^N \mathbb{C}^2$ that can be obtained from ρ by LOCC with some probability. This probability can be arbitrarily small as long as it is nonzero. This class of trans-

formations is called stochastic-LOCC (SLOCC). Each of these states $\tilde{\rho}$ is the normalized output of a separable (not necessarily trace-preserving) completely-positive map [1], with ρ as input:

$$\tilde{\rho} = \frac{\Omega(\rho)}{\text{tr } \Omega(\rho)}. \quad (2)$$

By separable map we mean one that can be written as

$$\Omega(\rho) = \sum_k [M_1^k \otimes \cdots \otimes M_N^k] \rho [M_1^k \otimes \cdots \otimes M_N^k]^\dagger, \quad (3)$$

with $M_n^k : \mathcal{H}_n \rightarrow \mathbb{C}^2$ for all k and $n = 1 \dots N$. We consider SLOCC transformations because we do not care about the rates at which the states $\tilde{\rho}$ can be obtained from ρ . Instead, we want to know which of the states $\tilde{\rho}$ resembles more to the GHZ-state. We quantify this resemblance by the fidelity that a state $\tilde{\rho}$ has with the N -partite GHZ state

$$|\Phi\rangle = \frac{1}{\sqrt{2}} (|0 \cdots 0\rangle + |1 \cdots 1\rangle). \quad (4)$$

Define $E(\rho)$ as the largest overlap with the GHZ that a state $\tilde{\rho}$ obtainable from ρ by SLOCC can achieve:

$$E(\rho) = \sup_{\Omega \in \text{SEP}} \frac{\text{tr} [\Omega(\rho) \Phi]}{\text{tr } \Omega(\rho)}, \quad (5)$$

where Φ is the projector onto the N -partite GHZ state (4), and the supremum is taken over all maps of the form (3) for which $\text{tr} [\Omega(\rho)] > 0$.

The reason for writing $E(\rho)$ as a supremum instead of a maximum is because, for some states ρ , the set of numbers $\{\text{tr}[\tilde{\rho}\Phi] : \tilde{\rho} \text{ obtainable from } \rho \text{ by SLOCC}\}$ does not have a maximum. In such cases, the probability of obtaining $\tilde{\rho}$ from ρ goes to zero as $\text{tr}[\tilde{\rho}\Phi]$ goes to $E(\rho)$. When $E(\rho) = 1$ this phenomenon is called quasi-distillation [6, 7]. In [9] it is shown that if $E(\rho) > 1/2$ one can asymptotically distill N -partite GHZ-states from ρ . In complement, $E(\rho) \geq 1/2$ holds for any ρ , because the state $|0 \cdots 0\rangle$ can be prepared locally and its fidelity with Φ is $1/2$. Therefore, the range of E is $[1/2, 1]$.

By definition (5), the quantity $E(\rho)$ is nonincreasing under SLOCC processing of ρ , and thus, an entanglement monotone [10]. It is also an operationally meaningful entanglement measure in the context of single-copy distillation: $E(\rho)$ is the probability that a state distilled from ρ “looks” like the GHZ state. In the bipartite case ($N = 2$), $E(\rho)$ is related to the average fidelity of the conclusive teleportation channel obtainable from ρ , denoted $F(\rho)$. In [7] it is shown that

$$F(\rho) = \frac{2E(\rho) + 1}{3}. \quad (6)$$

The quantity E also allows us to express our main result in a compact way.

III. RESULTS

Theorem 1. *An N -partite state σ is entangled if, and only if, for any $\lambda \in [1/2, 1)$ there exists an N -partite state ρ such that $E(\rho) \leq \lambda$ and $E(\rho \otimes \sigma) > \lambda$.*

In other words, chose a threshold λ on the “quality” of the distilled entanglement above which you are satisfied, and consider the set of states ρ from which it is impossible to distill such a sufficiently good entanglement $E(\rho) \leq \lambda$. Any entangled state σ (no matter how weakly entangled it is) can increase the “quality” of the entanglement distilled from some states ρ (in the above mentioned set) to a value larger than the threshold λ . In particular, if we choose a high threshold (e.g. $E(\rho) \leq 0.999$), any entangled state σ contributes by producing a result with even more purity ($E(\rho \otimes \sigma) > 0.999$). Then, one can argue that GHZ-like entanglement is being extracted form σ . Also remarkably, notice that σ could factorize with respect to some parties (or equivalently, σ is only shared by less than N parties), and yet, σ enhances the full N -partite GHZ-like entanglement present in other states! Hence, the way Theorem 1 generalizes the results proven in [4] is, unexpectedly, the strongest possible one. In what follows, we provide another surprising example.

Let us consider a three-qubit state σ_{shifts} , presented in [8], which has remarkable properties. The state σ_{shifts} is proportional to the projector onto the subspace orthogonal to the unextendible product basis $\{|0, 1, +\}, |1, +, 0\rangle, |+, 0, 1\rangle, |-, -, -\rangle\}$, where $\{|0\rangle, |1\rangle\}$ is an orthonormal basis and $|\pm\rangle = |0\rangle \pm |1\rangle$. This state is not fully-separable (1), but when any two of the three parties are considered as a single one, the resulting bipartite state becomes separable. This property may suggest that σ_{shifts} does not contain useful quantum correlations. Yet, according to Theorem 1, 3-partite GHZ-like entanglement can be extracted from σ_{shifts} , but also 4-partite GHZ-like entanglement, and so on.

One can generalize Theorem 1 to more intricate

single-copy distillation scenarios. We denote by S any subset of more than one party $S \subseteq \{1, \dots, N\}$, and by $|\Phi_S\rangle$ the $|S|$ -partite GHZ-state (4) shared among all parties in S . Consider M disjoint subsets of this kind S_1, \dots, S_M and a subset R containing the rest of parties: $R = \{1, \dots, N\} \setminus \bigcup_{m=1}^M S_m$. Suppose that the parties within each subset S_1, \dots, S_M aim at distilling a shared GHZ state, and the rest of parties R help to achieve this goal. This scenario motivates the definition of a quantity Q which generalizes E :

$$Q_{S_1 \dots S_M}(\rho) = \sup_{\Omega \in \text{SEP}} \frac{\text{tr} [\Omega(\rho) \mathbb{I}_R \otimes \Phi_{S_1} \otimes \dots \otimes \Phi_{S_M}]}{\text{tr} \Omega(\rho)}. \quad (7)$$

Clearly, $Q_{\{1, \dots, N\}} = E$. One can check that the range of $Q_{S_1 \dots S_M}$ is $[2^{-M}, 1]$. Theorem 1 can be generalized to this more intricate distillation scenario.

Theorem 2. *An N -partite state σ is entangled if, and only if, for any partition of the set of parties S_1, \dots, S_M, R and any $\lambda \in [2^{-M}, 1)$ there exists an N -partite state ρ such that $Q_{S_1 \dots S_M}(\rho) \leq \lambda$ and $Q_{S_1 \dots S_M}(\rho \otimes \sigma) > \lambda$.*

This result has a similar interpretation than Theorem 1, but its consequences are more rich. Imagine a 5-partite scenario where parties $\{1, 2\}$ want to distill a singlet $|\Phi_{\{1, 2\}}\rangle$, or any state whose fidelity with $|\Phi_{\{1, 2\}}\rangle$ is larger than 0.9. Parties $\{3, 4, 5\}$ share the supposedly useless state $\sigma_{\text{shifts}\{3, 4, 5\}}$. Theorem 2 demonstrates the existence of a 5-partite state $\rho_{\{1, \dots, 5\}}$ from which it is impossible to extract any state whose fidelity with $|\Phi_{\{1, 2\}}\rangle$ is larger than 0.9, but, together with $\sigma_{\text{shifts}\{3, 4, 5\}}$ this goal can be achieved. Notice that $\sigma_{\text{shifts}\{3, 4, 5\}}$ does not involve parties $\{1, 2\}$! Therefore, in the joint “activation” of $\rho_{\{1, \dots, 5\}}$ and $\sigma_{\text{shifts}\{3, 4, 5\}}$, some intricate teleportation-like phenomena between the sets of parties $\{1, 2\}$ and $\{3, 4, 5\}$ take place.

IV. PROOFS

In this section the core of the proofs of Lemmas 1 and 2 is included. The remaining part of the proofs can be found in the appendix.

Proof of Theorem 1. If σ is fully-separable then $E(\rho \otimes \sigma) = E(\rho)$ for any ρ . This holds because fully-separable states can be created by LOCC, and the definition of E already involves an optimization over LOCC. Let us prove the other direction of the equivalence.

From now on σ is an arbitrary N -partite not fully-separable state acting on $\mathcal{H} = \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_N$, and λ is fixed to some arbitrary value within $[1/2, 1)$. We have to show that there always exists a state ρ such that $E(\rho) \leq \lambda$ and $E(\rho \otimes \sigma) > \lambda$. We fix ρ to be an N -partite state for which the n^{th} party’s Hilbert space is $\mathcal{J}_n \otimes \mathcal{K}_n$, where $\mathcal{J}_n = \mathcal{H}_n$ and $\mathcal{K}_n = \mathbb{C}^2$, for $n = 1 \dots N$.

We also define $\mathcal{J} = \bigotimes_n^N \mathcal{J}_n$ and $\mathcal{K} = \bigotimes_n^N \mathcal{K}_n$.

Given a finite list of pairs of positive numbers $(x_1, y_1), \dots (x_n, y_n)$ the following inequality can be proven by induction:

$$\frac{x_1 + \dots + x_n}{y_1 + \dots + y_n} \leq \max_k \frac{x_k}{y_k}. \quad (8)$$

Using it, one can see that the the supremum in expression (5) is always achievable by a map Ω with only one term:

$$E(\rho) = \sup_{\mathbf{M}} \frac{\text{tr} [\mathbf{M} \rho \mathbf{M}^\dagger \Phi]}{\text{tr} [\mathbf{M} \rho \mathbf{M}^\dagger]}, \quad (9)$$

where \mathbf{M} is any product matrix $\mathbf{M} = M_1 \otimes \dots \otimes M_N$ with $M_n : [\mathcal{H}_n \otimes \mathbb{C}^2] \rightarrow \mathbb{C}^2$ for $n = 1 \dots N$. Using (9) one can characterize the set of states ρ satisfying $E(\rho) \leq \lambda$, by the following set of linear inequalities:

$$\text{tr} [\rho \mathbf{M}^\dagger (\lambda \mathbb{I} - \Phi) \mathbf{M}] \geq 0 \quad \forall \mathbf{M} = M_1 \otimes \dots \otimes M_N \quad (10)$$

where \mathbb{I} is the identity matrix acting on \mathcal{K} . For convenience, in the rest of the proof ρ is allowed to be not normalized. We denote by \mathcal{C} the set of states satisfying all the inequalities (10):

$$\mathcal{C} = \{\rho : \rho \geq 0, E(\rho) \leq \lambda\}, \quad (11)$$

which is a convex cone. The dual cone of \mathcal{C} is

$$\mathcal{C}^* = \{X : \text{tr} [\rho X] \geq 0 \forall \rho \in \mathcal{C}\}. \quad (12)$$

A generalized version of Farkas Lemma [11] states that any matrix $X \in \mathcal{C}^*$ can be written as

$$X = \sum_k \mathbf{M}_k^\dagger (\lambda \mathbb{I} - \Phi) \mathbf{M}_k + \sum_s P_s, \quad (13)$$

where P_s are positive matrices, and \mathbf{M}_k are arbitrary product matrices like in (10).

Let us concentrate on the condition $E(\rho \otimes \sigma) > \lambda$. Instead of computing the supremum in (9) we consider a particular filtering operation $\tilde{\mathbf{M}}$, with which we obtain a lower bound on $E(\rho \otimes \sigma)$. The chosen form of $\tilde{\mathbf{M}}$ is

$$\tilde{M}_n = \langle \phi_{\mathcal{H}_n \mathcal{J}_n} | \otimes \mathbb{I}_{\mathcal{K}_n} \quad n = 1 \dots N, \quad (14)$$

where $|\phi_{\mathcal{H}_n \mathcal{J}_n}\rangle$ is the (local) maximally entangled state between the systems corresponding to \mathcal{H}_n and \mathcal{J}_n (which have the same dimension), and $\mathbb{I}_{\mathcal{K}_n}$ is the identity matrix acting on \mathcal{K}_n . A little calculation shows that for any matrix Z acting on \mathcal{K} , the equality

$$\text{tr} [\tilde{\mathbf{M}} (\rho_{\mathcal{J} \mathcal{K}} \otimes \sigma_{\mathcal{H}}) \tilde{\mathbf{M}}^\dagger Z] = \nu \text{tr} [\rho_{\mathcal{J} \mathcal{K}} (\sigma_{\mathcal{J}}^\text{T} \otimes Z_{\mathcal{K}})] \quad (15)$$

holds, where σ^T stands for the transpose of σ , and $\nu > 0$. In the above expression the sub-indexes $\mathcal{H}, \mathcal{J}, \mathcal{K}$ explicitly indicate on which Hilbert spaces every matrix acts, and with which other matrices its indexes

are contracted. Using (15), a sufficient condition for $E(\rho \otimes \sigma) > \lambda$ is

$$\text{tr} [\rho (\sigma^\text{T} \otimes (\lambda \mathbb{I} - \Phi))] < 0. \quad (16)$$

Let us show that there always exists a $\rho \in \mathcal{C}$ satisfying this inequality, by creating a contradiction.

Suppose that no single $\rho \in \mathcal{C}$ satisfies (16). Then, by definition (12), the matrix $\sigma^\text{T} \otimes (\lambda \mathbb{I} - \Phi)$ belongs to \mathcal{C}^* , and we can express it as in (13). One way of writing this is

$$\sigma^\text{T} \otimes (\lambda \mathbb{I} - \Phi) - \Omega(\lambda \mathbb{I} - \Phi) \geq 0, \quad (17)$$

where Ω maps matrices acting on \mathcal{K} to matrices acting on $\mathcal{H} \otimes \mathcal{K}$, and is separable (3). In the rest of the proof we also use the same symbol Ω to denote any separable completely-positive map. This is not confusing because each of these maps is arbitrary, and the input and output spaces of each Ω is unambiguously fixed by the context. Performing the partial trace over \mathcal{H} to (17) we obtain

$$(\lambda \mathbb{I} - \Phi) - \Omega(\lambda \mathbb{I} - \Phi) \geq 0. \quad (18)$$

Notice that here Ω is different than in (17), but still separable. In [9] it was presented a depolarization protocol (here denoted by Δ) that can be implemented by LOCC, and leaves invariant the identity and the GHZ state: $\Delta(\mathbb{I}) = \mathbb{I}$ and $\Delta(\Phi) = \Phi$. Because Δ is a completely positive map, we can apply it to the left-hand side of (18) obtaining the positive matrix

$$(\lambda \mathbb{I} - \Phi) - [\Delta \circ \Omega \circ \Delta](\lambda \mathbb{I} - \Phi) \geq 0. \quad (19)$$

Lemma 1 in the Appendix shows that such an Ω must fulfill $(\lambda \mathbb{I} - \Phi) - [\Delta \circ \Omega \circ \Delta](\lambda \mathbb{I} - \Phi) = 0$. Hence, the trace of the left-hand side of (17) is zero, and a positive traceless matrix can only be the null matrix. Using the properties of Δ we can write

$$[(\mathbb{I}_{\mathcal{H}} \otimes \Delta_{\mathcal{K}}) \circ \Omega \circ \Delta](\lambda \mathbb{I} - \Phi) = \sigma^\text{T} \otimes (\lambda \mathbb{I} - \Phi). \quad (20)$$

Lemma 2 in the Appendix tells us that σ^T must be separable. But this is in contradiction with the initial assumption that σ is entangled. Therefore, the supposition that no single $\rho \in \mathcal{C}$ satisfies (16) is false. \square

Proof of Theorem 2. Here one proceeds in the same way as before, but instead, the depolarization protocol Δ is applied independently by each subset of parties S_m . In other words, one has to proceed with the global depolarization map $\Delta_{S_1} \otimes \dots \otimes \Delta_{S_M} \otimes \mathbb{I}_{\mathcal{R}}$. \square

V. FINAL REMARKS

The statement of Theorem 1 can be made stronger for the case $\lambda = 1/2$. The SLOCC operation (14)

that transforms $\rho \otimes \sigma$ into a state having fidelity with the GHZ larger than 1/2, can be substituted by a deterministic operation (LOCC). This is done by using the following trick. When the SLOCC operation (14) succeeds, the N parties do nothing, and when it fails they substitute the residual state by $|0 \cdots 0\rangle$, whose fidelity with the GHZ is 1/2. Clearly, the mixture of the success and failure states has fidelity with the GHZ strictly larger than 1/2. Therefore, all that we have said is not a particular fact of SLOCC transformations, everything can be done with probability one.

The method used to prove these theorems is non-constructive, hence it does not say much about the state ρ , whose entanglement is enhanced by σ . The only thing we know about ρ is that it is related to an entanglement witness [12] that detects σ . Precisely, the operator

$$W_{\mathcal{H}} = \text{tr}_{\mathcal{K}} [\rho_{\mathcal{H}\mathcal{K}} (\lambda \mathbb{I}_{\mathcal{K}} - \Phi_{\mathcal{K}})] , \quad (21)$$

can be proved to be an entanglement witness by imposing $E(\rho) \leq \lambda$. That W detects σ follows from inequality (16). As a consequence of Theorem 1, the set of witnesses of the form (21) is complete, in the sense that they detect all entangled states for any number of parties.

It is straightforward to generalize the depolarization protocol in [9] to larger local dimension ($d > 2$). This suggests that these theorems also hold when considering the overlap with the higher dimensional state

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^d |k \cdots k\rangle . \quad (22)$$

- [1] M. A. Nielsen, I. L. Chuang; *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
- [2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters; quant-ph/9604024.
- [3] M. Horodecki, P. Horodecki, R. Horodecki; Phys. Rev. Lett. **80**, 5239 (1998).
- [4] Ll. Masanes; Phys. Rev. Lett. **96**, 150501 (2006).
- [5] D. M. Greenberger, M. Horodecki, A. Zeilinger; *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*. Edited by M. Kafatos (Kluwer, Dordrecht, 1989).
- [6] P. Horodecki, M. Horodecki, R. Horodecki; Phys. Rev. Lett. **82**, 1056-1059 (1999).
- [7] M. Horodecki, P. Horodecki, R. Horodecki; quant-ph/9807091.
- [8] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, B. M. Terhal; Phys. Rev. Lett. **82**, 5385 (1999).
- [9] W. Dür, J. I. Cirac; Phys. Rev. A **61**, 042314 (2000).
- [10] G. Vidal; J. Mod. Opt. **47**, 355 (2000).
- [11] B. D. Craven, J. J. Koliha; SIAM J. Math. Anal. **8**, pp. 983 (1977).

It would be interesting to know if Theorem 1 can be generalized when the fidelity is measured with respect to an arbitrary entangled pure-state, or contrary, there are states for which such a theorem does not hold. That would provide deep insights on the structure of multipartite entanglement.

VI. CONCLUSIONS

We have shown that all entangled states can increase the “quality” of the entanglement distillable from a single-copy of other states. Obviously this task is impossible for fully-separable states. Hence, all quantum correlations have a qualitatively different character. Then we can say more than “entanglement is a physical resource”; we can say that “*all* entanglement is a physical resource”!

VII. ACKNOWLEDGMENTS

The author is thankful to Fernando Brandão, Aram Harrow and Andreas Winter for useful discussions. This work has been supported by the UK EPSRC’s “IRC QIP”, and the EU project QAP IST-3-015848.

- [12] M. Lewenstein, B. Kraus, J. I. Cirac, P. Horodecki; quant-ph/0005014.
- [13] A. Jamiołkowski; Rep. Mod. Phys. **3**, 275 (1972).
- [14] www.iwr.uni-heidelberg.de/groups/comopt/software/PORTA
- [15] W. Fulton, J. Harris; *Representation Theory, a first course* (Springer).

APPENDIX A: PROOFS OF LEMMAS 1 AND 2

In this appendix we describe the depolarization map Δ used in the proofs, and find some of its properties. We use the same notation as in the rest of the paper: $\mathcal{H} = \bigotimes_n^N \mathcal{H}_n$, $\mathcal{K} = \bigotimes^N \mathbb{C}^2$, and Ω is any separable completely-positive map whose input and output spaces become fixed by the context. We also show the following two lemmas, which are necessary for proving Theorems 1 and 2.

Lemma 1. *Let Ω be any separable map (3) transforming matrices acting on \mathcal{K} to matrices acting on \mathcal{K} ,*

and $\lambda \in [1/2, 1]$, then

$$[\Delta \circ \Omega \circ \Delta](\lambda \mathbb{I} - \Phi) \leq \lambda \mathbb{I} - \Phi \quad (\text{A1})$$

implies

$$[\Delta \circ \Omega \circ \Delta](\lambda \mathbb{I} - \Phi) = \lambda \mathbb{I} - \Phi. \quad (\text{A2})$$

Lemma 2. *Let Ω be any separable map (3) transforming matrices acting on \mathcal{K} to matrices acting on $\mathcal{H} \otimes \mathcal{K}$, and $\lambda \in [1/2, 1]$, then*

$$[(\mathbb{I}_{\mathcal{H}} \otimes \Delta_{\mathcal{K}}) \circ \Omega \circ \Delta](\lambda \mathbb{I} - \Phi) = \sigma \otimes (\lambda \mathbb{I} - \Phi) \quad (\text{A3})$$

implies that σ is separable (1).

1. Notation

Denote by \mathbf{x} the N -bit string $x_1 x_2 \dots x_N$ where $x_n \in \{0, 1\}$, by $\bar{\mathbf{x}}$ the N -bit string where each bit has the opposite value as in \mathbf{x} , and by $|\mathbf{x}\rangle$ the vector $|x_1\rangle \otimes \dots \otimes |x_N\rangle \in \mathcal{K}$, where $\{|0\rangle, |1\rangle\}$ is an orthonormal basis of \mathbb{C}^2 . The N -partite GHZ basis is defined as

$$|\Phi_{\mathbf{x}}^{\pm}\rangle = \frac{1}{\sqrt{2}} (|\mathbf{x}\rangle \pm |\bar{\mathbf{x}}\rangle) \quad \forall \mathbf{x} \text{ even}, \quad (\text{A4})$$

where \mathbf{x} even means that $x_N = 0$. There are 2^N such vectors and all of them are orthogonal. (We impose \mathbf{x} to be even in order not to doubly count states.) We also define the unit-trace, positive semi-definite matrices

$$P_{\mathbf{x}} = \frac{1}{2} (|\mathbf{x}\rangle\langle\mathbf{x}| + |\bar{\mathbf{x}}\rangle\langle\bar{\mathbf{x}}|) \quad \forall \mathbf{x} \text{ even}, \quad (\text{A5})$$

$$P_{\pm} = |\Phi_{\mathbf{x}}^{\pm}\rangle\langle\Phi_{\mathbf{x}}^{\pm}|. \quad (\text{A6})$$

In the next, the index r takes values in the set $\{+, -, 2, 4, 6, 8, \dots, 2^N - 2\}$ and is used to label the states P_r . For instance, one can write $\mathbb{I} = 2 \sum_r P_r - P_+ - P_-$.

2. Depolarization protocol

In [9] it is presented a useful LOCC protocol that transforms N -qubit states. The protocol is implemented through the following $(N+1)$ steps: (step 1) with probability $1/2$ the N parties apply $\bigotimes_x \sigma_x$ and with probability $1/2$ they do nothing, (step 2) with probability $1/2$ parties $\{1, N\}$ apply $\sigma_z \otimes \sigma_z$ and with probability $1/2$ they do nothing, (step 3) with probability $1/2$ parties $\{2, N\}$ apply $\sigma_z \otimes \sigma_z$ and with probability $1/2$ they do nothing, ... (step N) with probability $1/2$ parties $\{N-1, N\}$ apply $\sigma_z \otimes \sigma_z$ and with probability $1/2$ they do nothing, (step $N+1$) the N

parties apply $\bigotimes_n \sigma_z^{y_n}$, where y_2, y_3, \dots, y_N are independent (uniformly distributed) random bits, and $y_1 = \sum_{n=2}^N y_n \bmod 2$. Let Δ be the completely-positive map corresponding to this protocol. Because this protocol can be implemented by LOCC the map Δ is trace-preserving and separable. It is easy to check that for any N -qubit state ϱ (acting on \mathcal{K})

$$\Delta(\varrho) = \sum_r \varrho_r P_r, \quad (\text{A7})$$

$$\varrho_{\pm} = \text{tr}(P_{\pm} \varrho), \quad (\text{A8})$$

$$\varrho_{\mathbf{x}} = 2 \text{tr}(P_{\mathbf{x}} \varrho) \quad \forall \mathbf{x} \text{ even}. \quad (\text{A9})$$

3. Characterization of $[\Delta \circ \Omega \circ \Delta]$ -maps

Let Ω be a separable completely-positive map that transforms N -qubit states into N -qubit states. By the Jamiołkowski theorem [13] we can write $\Omega(Z) = \text{tr}_{\mathcal{K}}(\Theta_{\mathcal{K}'\mathcal{K}} Z_{\mathcal{K}}^{\text{T}})$ for any Z acting on \mathcal{K} , where $\Theta_{\mathcal{K}'\mathcal{K}}$ is a fully-separable N -partite state with two qubits per site. The N -qubit Hilbert space \mathcal{K} (\mathcal{K}') corresponds to the input (output) of the channel Ω . One can check that

$$[\Delta \circ \Omega \circ \Delta](Z) = \text{tr}_{\mathcal{K}}([\Delta_{\mathcal{K}'} \otimes \Delta_{\mathcal{K}}](\Theta_{\mathcal{K}'\mathcal{K}}) Z_{\mathcal{K}}^{\text{T}}), \quad (\text{A10})$$

which, according to (A7), implies that the state Θ associated to the map $[\Delta \circ \Omega \circ \Delta]$ is of the form

$$\Theta = \sum_{r,r'} \Theta_{rr'} P_r \otimes P_{r'}, \quad (\text{A11})$$

$$\Theta_{rr'} \geq 0 \quad \forall r, r'. \quad (\text{A12})$$

Because the maps Ω and Δ are fully-separable, the state Θ must be PPT with respect to all bipartitions of the N parties [9]. Denote by ϱ^{T_S} the matrix obtained when transposing in the basis $\{|0\rangle, |1\rangle\}$ of the Hilbert spaces of the parties $S \subseteq \{1, \dots, N\}$ the matrix ϱ . One can check that for any $S \subseteq \{1, \dots, N\}$

$$P_{\pm}^{T_S} = P_0 \pm \frac{1}{2} (|\mathbf{x}_S\rangle\langle\bar{\mathbf{x}}_S| + |\bar{\mathbf{x}}_S\rangle\langle\mathbf{x}_S|), \quad (\text{A13})$$

$$P_{\mathbf{x}}^{T_S} = P_{\mathbf{x}}, \quad (\text{A14})$$

where \mathbf{x}_S is the N -bit string with $x_n = 1$ if $n \in S$ and $x_n = 0$ otherwise, for $n = 1, \dots, N$. Without loss of generality we assume that S never contains the N^{th} party, or equivalently, the number with binary expansion \mathbf{x}_S is even. Using (A13, A14) one can obtain the necessary and sufficient condition for a state of the form (A11) to be PPT for all subsets of parties S , which is:

$$|\Theta_{++} - \Theta_{+-} + \Theta_{-+} - \Theta_{--}| - \Theta_{+\mathbf{x}} - \Theta_{-\mathbf{x}} \leq 0 \quad (\text{A15})$$

$$|\Theta_{++} + \Theta_{+-} - \Theta_{-+} - \Theta_{--}| - \Theta_{\mathbf{x}+} - \Theta_{\mathbf{x}-} \leq 0 \quad (\text{A16})$$

$$|\Theta_{+x} - \Theta_{-x}| - \Theta_{xx'} \leq 0 \quad (\text{A17})$$

$$|\Theta_{x+} - \Theta_{x-}| - \Theta_{xx'} \leq 0 \quad (\text{A18})$$

$$|\Theta_{+x} - \Theta_{-x} + \Theta_{x+} - \Theta_{x-}|$$

$$- \Theta_{++} + \Theta_{+-} + \Theta_{-+} - \Theta_{--} - \Theta_{xx} \leq 0 \quad (\text{A19})$$

$$|\Theta_{+x} - \Theta_{-x} - \Theta_{x+} + \Theta_{x-}|$$

$$+ \Theta_{++} - \Theta_{+-} - \Theta_{-+} + \Theta_{--} - \Theta_{xx} \leq 0 \quad (\text{A20})$$

for all $\mathbf{x}, \mathbf{x}' \in \{2, 4, 6, 8, \dots, 2^N - 2\}$ with $\mathbf{x}' \neq \mathbf{x}$.

4. Proof of Lemma 1

If we represent the Jamiołkowski state associated to the map $[\Delta \circ \Omega \circ \Delta]$ as (A11), equation (A1) is equivalent to the following set of inequalities

$$\lambda - 1 - \lambda \sum_r \Theta_{+r} + \Theta_{++} \geq 0, \quad (\text{A21})$$

$$\lambda - \lambda \sum_r \Theta_{-r} + \Theta_{-+} \geq 0, \quad (\text{A22})$$

$$2\lambda - \lambda \sum_r \Theta_{xr} + \Theta_{x+} \geq 0, \quad (\text{A23})$$

for all \mathbf{x} even. Now, for each $N \geq 2$ and $\lambda \in [1/2, 1]$, the set of inequalities (A12,A15-A23) defines a linear-programming feasibility problem. Notice that each inequality written with an absolute value is equivalent to two plain linear inequalities. Fixing N and λ to some values, one can obtain the polyhedron that contains all solutions (for example with the software [14]). We have done this for different values of N and λ , obtaining always the polyhedron consisting of the single point

$$\Theta_{rr'}^{\text{sol}} = \begin{cases} 1 & \text{if } r = r' = \pm \\ 2 & \text{if } r = r' \in \{2, 4, 6, \dots, 2^N - 2\} \\ 0 & \text{otherwise} \end{cases} \quad (\text{A24})$$

This is precisely the Jamiołkowski state corresponding to the depolarization map Δ :

$$\Theta^{\text{sol}} = P_+ \otimes P_+ + P_- \otimes P_- + 2 \sum_{\mathbf{x}} P_{\mathbf{x}} \otimes P_{\mathbf{x}}. \quad (\text{A25})$$

In the next, we show that Θ^{sol} is indeed the unique solution for any value of λ and N .

By exploiting the symmetry of equations (A12, A15-A23) one can get a system of 25 linear inequalities and 10 unknowns, for any value of $N \geq 2$. Consider the set of permutations $\{\pi\}$ that leave invariant the first two elements in $(+, -, 2, 4, 6, \dots, 2^N - 2)$. If we perform the transformation $\Theta_{rr'} \rightarrow \Theta_{\pi_r \pi_{r'}}$ the system of inequalities (A12,A15-A23) remains invariant. Therefore, if $\tilde{\Theta}_{rr'}$ is a solution then also $\tilde{\Theta}_{\pi_r \pi_{r'}}$ is a solution, for any permutation π of the kind specified above. Because the set of inequalities (A12, A15-A23) is linear, convex combinations of

solutions are also solutions. Hence, given a solution $\tilde{\Theta}_{rr'}$ we can always generate another solution of the form

$$\Theta_{rr'}^{\text{inv}} = \frac{1}{(2^{N-1} - 1)!} \sum_{\pi} \tilde{\Theta}_{\pi_r \pi_{r'}}, \quad (\text{A26})$$

where the sum is over the group of permutations specified above. It is clear that the result of this average is invariant under transformations of the form $\Theta_{rr'}^{\text{inv}} \rightarrow \Theta_{\pi_r \pi_{r'}}^{\text{inv}}$. Therefore, the coefficients $\Theta_{\pm\pm}^{\text{inv}}$ do not depend on the value of \mathbf{x} , and analogously for $\Theta_{\pm x}^{\text{inv}}$. By applying group theoretic arguments [15] one can see that the coefficients of the form $\Theta_{xx'}^{\text{inv}}$ only depend on whether $\mathbf{x} = \mathbf{x}'$ or $\mathbf{x} \neq \mathbf{x}'$. To see this, consider the representation of $\{\pi\}$ as orthogonal matrices which permute the components of vectors accordingly: $O_{\mathbf{x}\mathbf{x}'} = \delta_{\mathbf{x}'\pi_{\mathbf{x}}}$. This representation decomposes into two irreducible ones: (i) the trivial representation spanned by the vector with all the entries equal to one ($v_{\mathbf{x}} = 1 \forall \mathbf{x}$), and (ii) the so called *standard* representation [15], corresponding to the complementary subspace. By Schur's Lemma [15], any matrix that commutes with all members of the group $\{O_{\mathbf{x}\mathbf{x}'}\}$ has to be a linear combination of the projector onto $v_{\mathbf{x}}$ and the identity. Hence, the restriction of the matrix $\Theta_{rr'}^{\text{inv}}$ to $r, r' \in \{2, 4, \dots, 2^N - 2\}$ can be expressed as $\Theta_{xx'}^{\text{inv}} = \alpha + \beta \delta_{\mathbf{x}\mathbf{x}'}$, where α and β are two numbers. Concluding, each invariant state $\Theta_{rr'}^{\text{inv}}$ is completely characterized by 10 real numbers: $\Theta_{++}, \Theta_{+-}, \Theta_{-+}, \Theta_{--}, \Theta_{+2}, \Theta_{-2}, \Theta_{2+}, \Theta_{2-}, \Theta_{22}$ and Θ_{24} . (The choice of 2 and 4 as distinct even numbers is irrelevant.)

Now, we can rewrite the set of inequalities (A12,A15-A23) with only these 10 numbers:

$$\Theta_{++}, \Theta_{+-}, \Theta_{-+}, \Theta_{--} \geq 0 \quad (\text{A27})$$

$$\Theta_{+2}, \Theta_{-2}, \Theta_{2+}, \Theta_{2-}, \Theta_{22}, \Theta_{24} \geq 0 \quad (\text{A28})$$

$$|\Theta_{++} - \Theta_{+-} + \Theta_{-+} - \Theta_{--}| - \Theta_{+2} - \Theta_{-2} \leq 0 \quad (\text{A29})$$

$$|\Theta_{++} + \Theta_{+-} - \Theta_{-+} - \Theta_{--}| - \Theta_{+2} - \Theta_{-2} \leq 0 \quad (\text{A30})$$

$$|\Theta_{+2} - \Theta_{-2}| - \Theta_{24} \leq 0 \quad (\text{A31})$$

$$|\Theta_{+2} - \Theta_{-2}| - \Theta_{24} \leq 0 \quad (\text{A32})$$

$$|\Theta_{+2} - \Theta_{-2} + \Theta_{2+} - \Theta_{2-}| + \quad (\text{A33})$$

$$- \Theta_{++} + \Theta_{+-} + \Theta_{-+} - \Theta_{--} - \Theta_{22} \leq 0$$

$$|\Theta_{+2} - \Theta_{-2} - \Theta_{2+} + \Theta_{2-}| + \quad (\text{A34})$$

$$+ \Theta_{++} - \Theta_{+-} - \Theta_{-+} + \Theta_{--} - \Theta_{22} \leq 0$$

$$\lambda (\Theta_{++} + \Theta_{+-} + g_N \Theta_{+2}) - \Theta_{++} - 1 + \lambda \leq 0 \quad (\text{A35})$$

$$\lambda (\Theta_{-+} + \Theta_{--} + g_N \Theta_{-2}) - \Theta_{-+} - \lambda \leq 0 \quad (\text{A36})$$

$$\leq 0$$

$$\lambda (\Theta_{+2} + \Theta_{-2} + (g_N - 1) \Theta_{24} + \Theta_{22}) - \Theta_{+2} - 2\lambda \leq 0 \quad (\text{A37})$$

For any N , this system has 10 unknowns, but the coefficient $g_N = 2^{N-1} - 1$ still depends on N . By direct substitution one can check that the point Θ^{sol} in (A24) is a solution of this system. Let us prove that it is unique. If a new linear inequality can be expressed as a linear combination with non-negative coefficients of the inequalities (A27-A37), then it must be satisfied by all the solutions of this system. With the help of a computer, we have expressed each of the following 20 inequalities

$$\begin{aligned} 1 &\leq \Theta_{++}, \Theta_{--} \leq 1 \\ 2 &\leq \Theta_{22} \leq 2 \\ 0 &\leq \Theta_{+-}, \Theta_{-+}, \Theta_{+2}, \Theta_{-2}, \Theta_{2+}, \Theta_{2-}, \Theta_{24} \leq 0 \end{aligned}$$

as a linear combination with non-negative coefficients of the ones in (A27-A37), with the coefficients explicitly depending on g_N and λ . These coefficients are well defined for any $N \geq 2$ and $\lambda \in (1/2, 1)$, but unfortunately, some of them become singular when $\lambda = 1/2$. Later we analyze this case. This implies that, when $\lambda \neq 1/2$, all the solutions of (A27-A37) satisfy these inequalities, but it is straightforward to see that the only point satisfying them is Θ^{sol} , as we wanted to prove.

For $\lambda = 1/2$ and $N = 2$ we have solved the polyhedron (A27-A37) with the software [14]. In this case the set of solutions form a convex cone with vertex in Θ^{sol} . The software [14] also outputs the generators of the cone, which can be written as $\Theta^{[r]} = P_r \otimes (P_+ + P_-)$, for all r . Then, all the solutions are of the form $\Theta^{\text{cone}} = \Theta^{\text{sol}} + \sum_r \tau_r \Theta^{[r]}$ with $\tau_r \geq 0$. Because $\Theta_{+2}, \Theta_{-2}, \Theta_{24}, g_N, \lambda \geq 0$, and g_N increases with N , all solutions of (A27-A37) for any $N > 2$

are contained in the set of solutions for $N = 2$, denoted $\{\Theta^{\text{cone}}\}$. All points in $\{\Theta^{\text{cone}}\}$ have the property that $\Theta_{+2} = \Theta_{-2} = \Theta_{24} = 0$, therefore, increasing the value of g_N does not reduce the set of solutions. Thus, for any N , the set of solutions of (A27-A37) is precisely $\{\Theta^{\text{cone}}\}$. When $\lambda = 1/2$ we have that $\text{tr}[(P_+ + P_-)(\lambda \mathbb{I} - P_+)] = 0$, then all the maps in $\{\Theta^{\text{cone}}\}$ give the output $(\lambda \mathbb{I} - P_+)$ when the input is $(\lambda \mathbb{I} - P_+)$. Concluding, any Ω for which (A1) holds is such that (A2) must hold too. \square

5. Proof of Lemma 2

Applying Schur's Lemma [15] on the outer depolarization map $\Delta_{\mathcal{K}}$, if Ω maps states acting on \mathcal{K} to states acting on $\mathcal{H} \otimes \mathcal{K}$ then

$$\begin{aligned} [(\mathbb{I}_{\mathcal{H}} \otimes \Delta_{\mathcal{K}}) \circ \Omega \circ \Delta](\lambda \mathbb{I} - \Phi) &= \quad (A38) \\ (\lambda - 1) \sigma_+ \otimes P_+ + \lambda \sum_{r \neq +} \sigma_r \otimes P_r, \end{aligned}$$

where σ_r are unit-trace, positive semi-definite matrices acting on \mathcal{H} . Because the maps Δ, Ω and the states P_x are fully-separable, the states $\sigma_x = \text{tr}_{\mathcal{K}}[(\mathbb{I}_{\mathcal{H}} \otimes \Delta_{\mathcal{K}}) \circ \Omega \circ \Delta](P_x)$ must be fully-separable too, for $x \in \{2, 4, \dots, 2^N - 2\}$. The matrix $\sigma \otimes (\lambda \mathbb{I} - P_+)$ is product, and according to (A3) is equal to the right-hand side of (A38). This, together with the fact that the matrices P_r are orthogonal (with respect to the Hilbert-Schmidt scalar product), implies that all the matrices σ_r must be equal. Then $\sigma = \sigma_x$, which is fully-separable. \square